XI. FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 2006. március 24-25.

KVANTUMMECHANIKAI EFFEKTUSOK ALKALMAZÁSA AZ INFORMATIKAI BIZTONSÁGTECHNIKÁBAN

Árendás Csaba, Pethő László

Abstract

The importance of dependable security in up-to-date IT solutions is gaining more critical importance each day. A strict policy accompanied by continuously monitored traffic is required to avoid threats by the use of the latest technology. With increasing significance the protection of knowledge and expertise needs to be accomplished by well-planned theoretical basics implemented. IT security is a field where total safety cannot even be guaranteed, although the difficulty of intrusion and the amount of obstacles can be extremely increased. The realisation of the device is a hardware accessory which can produce a true random resource, accessible by any kind of operating system on kernel-level. Specific driver software will be created keeping in mind the ease of use. The physical generation is maintained by a specific circuit, to manage the work of the detector by only using the computer as an energy resource. The management of the connectivity, buffering, storing and the processing of the random data stream is controlled by an integrated microchip. All electronic and programmed material will be open source and available without restraints to reach the highest level of user trust.

Absztrakt

Napjaink informatikai rendszereivel kapcsolatban egyre nagyobb hangsúly helyeződik a biztonság kérdésére. Az információlopások, visszaélések ellen csak nagyon éber biztonságpolitikával és jól megalapozott technológiával léphetünk fel. Egyre fontosabb, hogy anyagi és szellemi értékeinket ne csak egy könnyen kikerülhető védelemre bízuk, hanem a védelem lényege komoly elméleti alapokon nyugaljon, így megakadályozhassuk, hogy a leleményes hackerek ügyes trükkökkel kijátszhassák azt. Az informatikai biztonság tipikusan az a terület, ahol 100%-os sebezhetetlenséget garantálni nem lehet, de megfelelő matematikai és fizikai apparátussal nagymértékben megnehezíthető a támadó dolga. A tervezett berendezés USB porton csatlakoztatható a számítógéphez, vagy

tetszőleges hordozható eszközhöz, például PDA-hoz. Ehhez megfelelő illesztőprogramokat készítünk több operációs rendszerhez is. Ha az átlagos felhasználóban nem is, de a szakképzett profiban biztosan felmerül, hogy a megvásárolt eszköz tényleg a specifikációnak megfelelően működik-e, nem ál-véletlenszámokat generál-e, így kompromittálva rendszere biztonságát. Hogy meggyőzzük a hozzáértő réteget, *teljesen nyíltá* és bárki számára elérhetővé tesszük a rendszer specifikációját az Interneten és mellékeljük minden egyes eladott termék mellé. Annak ellenére, hogy a vásárló nem tud meggyőződni a hardver eszköz belső működéséről, a nyílt szoftveres illesztő modulhoz vagy driverhez hozzáférhet.

A kutatás háttere

A fizika jelenlegi állása szerint a világunk alapjaiban véve nem írható fel egy egységes egyenlettel, mert a legelemibb kölcsönhatások véletlenszerűen történnek (például egy elektron pontos helye és sebessége igazi véletlen, elvileg is kiszámíthatatlan). Ezt a fizikai, *legelemibb* véletlent szeretnénk a kvantummechanikai világból felhasználni. Biztonságtechnikai felhasználásnál fontos követelmény, hogy más ne tudja lemérni az általunk detektált véletlent és ne is tudja azt módosítani. Számos hardver véletlenszám-generátor az éterből meríti a véletleneket; a termikus, vagy nagyfrekvenciás zaj ugyan jó forrás, de könnyen befolyásolható és lehallgatható.

Egy tökéletes véletlenszám-generátort számítógéppel megvalósítani nem lehetséges, hiszen a generált bitek nem lehetnek tökéletesen függetlenek, mert azok egy algoritmus egymást követő kimenetei, mely mindenképpen determinisztikus. Számítógéppel tehát nem állíthatóak elő valódi véletlen bitek, ezért a gépek által generált kvázi-véletlen számokat elnevezték álvéletlen (pseudo-random) számoknak. Az on-line titkosított adatcserék egyik sarkalatos pontja azonban a véletlenszám-generálás kérdése. Egy titkosított adatkapcsolat folyamán nagyon sok véletlenszámra van szükség, ami időlegesen a jelszavunkat helyettesítheti. Ha ezek nem eléggé véletlenek (megjósolhatóak, nem egyenletes az eloszlásuk), használhatunk bármilyen erős titkosítást, a szűk keresztmetszet ez lesz, így könnyen feltörhetővé válik. Mivel a számítógépet ösödök óta arra tervezték, hogy determinisztikusan, szabályszerűen működjön, ezért nagy probléma, hogy honnan veszünk igazi véletlent egy ilyen matematikai elvek szerint működő rendszerben. Ha „rosszul választunk”, vagyis nem igazi véletlenekkel dolgozunk, nagy az esélye annak, hogy a támadó megtippeli, kikövetkezteti a választásunkat. Ez olyan, mintha a jelszavunkat fejtené meg és így hozzáférhet, vagy akár módosíthatja féltve őrzött adatainkat.

Megvalósítás

A céltermék kisméretű eszköz, amely a számítógép USB portjára csatlakoztatható. A kvantummechanikai effektus megvalósításához magfizikai folyamatokat kívánunk felhasználni, valamint azok mérését implementálni. A kutatás alapját képezi a megfelelő folyamat kiválasztása, a méréshez szükséges eszközök és források megfelelő megválasztása, valamint azok számítógépes környezetbe való integrálása.

A technikai tervezés folyamán igyekeztünk elkerülni a biztonságtechnikai rendszereknél gyakran tapasztalt hibás, „*security by obscurity*” elvet [1]. A gyakori hiba, hogy a gyártó, illetve tervező titokban tartja rendszere forráskódját, nem enged bepillantást harmadik fél számára. Ezzel nagyon megnehezíti az esetleges hibák felszínre kerülésének lehetőségét, valamint bizalmatlanságot kelt a felhasználókban. Manapság alapelveként fogalmazható meg, hogy csak nyíltan, publikusan elérhető forráskódú titkosító, pszeudovéletlen-generáló algoritmust ajánlatos használni. Az algoritmus biztonságának, jóságának, vagyis nehezen feltörhetőségének nem szabad függenie az algoritmus titkosságától, hanem csak a tényleges titoktól, a kulcstól. Még ha a támadó hozzá is fér az eszköz teljes technikai és tervezői dokumentációjához, nem szabad, hogy ezzel bármiféle előnyhöz jusson és könnyebben kijátszhassa a védelmet. A hardveres véletlenszám-generálás is felveti ezt a problémát, hiszen a legtöbb felhasználó nem tud meggyőződni a fekete doboz tartalmáról; joggal félhet attól, hogy egy álvéletlenszám-generátort vásárolt.

Hasonló megoldások

Az optikai elven működő véletlenszám-generátorok [2] az egyes fotonok kvantummechanikai tulajdonságait használják fel. A fénysebességgel haladó fotonok esetén nem beszélhetünk helyről, csupán adott térrészben való megtalálási valószínűségről. Ez a tulajdonság használható ki, féligáteresztő tükrön való szóródással és irány szerinti detektálással. A terület aktív kutatási fázisban van. A legkomolyabb kihívást egy darab foton precíz detektálása jelenti; a jelenlegi megvalósítások egy közelítő beütésszám által keltett hatás után átlagolnak, emiatt a kész eszközök működési elve még megkérdőjelezhető, bár a teszteken már szép eredményeket mutatnak. Előnyük a fény tulajdonságaiból eredő nagy sebesség és a befolyásolhatatlanság. Jelenlegi hátrány a precíz berendezések hiánya, vagy azok hatalmas mérete és energiaigényes felépítése. Ezekben a generátorokban a kvantummechanika egy másik elve van implementálva. Kihasználják a fény sebességéből eredő teljes lokális meghatározhatatlanságot egy féligáteresztő tükör segítségével. Mivel a foton fénysebességgel halad, így a határozatlansági relációkból következik, hogy a pontos hely nem definiálható. A tükrön 50% valószínűséggel visszaverődik egy foton; vagy térítetlenül továbbhalad. A tükör két oldalára detektort helyezve és a fotonokat detektálva kaphatunk véletlen adatsort. Megjegyzendő, hogy ebben az esetben is axiomatikus megfontolásokról van szó. Az egyik detektort 1-el, a másikat 0-val jelölve minden egyes eseményhez rendelhetünk egy darab bitet, amely már nyers adatfolyamként is használható.

Számos elektronikai alkatrészben figyelhetők meg termikus effektusok, vagyis hőmérsékleti hatásra bekövetkező szerkezeti változások által a kimeneten okozott, a jelben mérhető változások. Ilyen például az egyszerű termikus zaj, vagy tranzisztorok esetében a munkapont-ingadozás; számtalan példát fel lehet sorolni. Ilyen áramkörök megépítése kis gyakorlattal gyors és egyszerű. Legfőbb hátrányuk az érzékenységük és befolyásolhatóságuk. A legtöbb ilyen eszköz a hőmérséklet kis emelésére vagy csökkentésére már a generált adatsor számottevő, vagy esetenkénti teljes romlásával reagál. Más

eszközökkel, például a mobiltelefonok által generált elektromágneses térrel is könnyedén megzavarhatóak. Mindezek ellenére számos eszköz kihasználja a termikus effektust véletlenek generálására [3,4,5].

Következmények

Rendkívüli veszteséget okozhat egy cég életében, ha a hálózat bármely pontján megsérül a biztonság. Ezt elkerülendő a vállalatok az üzletmenet megszakadásának elkerülésére, a fenyegető kockázatok tudatos felismerésére és a változásokhoz való gyorsabb alkalmazkodásra törekcszenek. A biztonságos gazdasági környezet mérhető üzleti előnyei mindenekelőtt a költségcsökkentés, a védettségs és a hatékonyság. A direktten erre a területre irányuló, ezzel közvetlen kapcsolatos bűncselekmények és azok lehetőségének csökkenése is az eszköz folyamatos használatának alapvető és természetes következménye. A szakirodalomban jónéhány véletlenszám-generálásra alapozó sikeres és sikertelen betörési kísérlet ismert (pl. a Netscape böngésző titkosítási hibája).

Ezúton szeretnénk köszönetet mondani a BME Általános és Analitikai Tanszéknek a kutatás lehetőségének biztosításáért és a szükséges eszközök rendelkezésre bocsátásáért; valamint az oktatóknak a személyes segítség nyújtásáért és támogatásáért.

Referenciák

- [1] Bruce Schneier: Applied Cryptography, John Wiley & Sons, 1995 december
- [2] ID Quantique: Optical Quantum Random Number Generator
<http://www.idquantique.com/products/quantis.htm>
- [3] HG400 Random Number Generator
<http://www.random.com.hr/products/hg400/>
- [4] Protego R200-USB TRNG
http://www.protego.se/sg200_d.htm
- [5] ComScire J1000KU RNG
<http://comscire.com/Products/J1000KU/>

Árendás Csaba / tanszéki demonstrátor
BME Általános és Analitikai Kémia Tanszék
+3670-242-7069; arendas@sch.bme.hu

Pethő László / hallgató
BME Természettudományi Kar, Mérnök-fizikus szak
+3670-204-4739; pl308@hszk.bme.hu